1. Report Security Classification: UNCLASSIFIED	

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
          JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol:
          C
	7. Address: NAVAL WAR COLLEGE
	          686 CUSHING ROAD
	          NEWPORT, RI 02841-1207

8. Title (Include Security Classification): ORGANIZING FOR INFORMATION OPERATIONS WITHIN THE JOINT TASK FORCE

9. Personal Authors: Major Lawrence W. McLaughlin, USAF

10.Type of Report: FINAL	**11. Date of Report**: 3 February 2003

12.Page Count: 20	**12A Paper Advisor (if any):Lt Col John Brence**

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:
Information in war, Information Operations, Command and control, Joint Task Force, PSYOP, JPOTF

15.Abstract:

Information operations (IO) continue to rise in prominence as a force multiplier for the joint force. Joint doctrine defines information operations as a broad range of capabilities and related activities that include operations security, psychological operations, electronic warfare, physical attack/destruction and special information operations. Given the importance and scope of IO across the spectrum of conflict, it would be logical that a robust organizational structure would be prescribed to support the multiple functions of IO and ensure the necessary coordination required to implement a comprehensive IO campaign. Unfortunately, this is not the case. Joint doctrine inadequately integrates IO into the Joint Task Force (JTF) organization to address the many aspects of IO. The current doctrinal organization for the conduct of IO – the IO cell – does not provide for unity of command or centralized planning necessary to support the commander's IO effort. A potential solution to this problem is to create a new organization within the JTF command and control structure modeled after the Joint Psychological Operation Task Force (JSOTF). This would greatly increase the ability of the Joint Force Commander to plan and execute a comprehensive IO campaign that is integrated with, and complementary to, the overall campaign plan.

16.Distribution / Availability of Abstract:	Unclassified **X**	Same As Rpt	DTIC Users

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461	**20.Office Symbol:** C

Security Classification of This Page **Unclassified**

NAVAL WAR COLLEGE
Newport, R.I.

ORGANIZING FOR INFORMATION OPERATIONS WITHIN
THE JOINT TASK FORCE

By

Lawrence W. McLaughlin
Major, USAF

A paper submitted to the Faculty of the Naval War College in partial satisfaction of
The requirements of the Department of Joint Military Operations

Signature: _____

February 3, 2003

Abstract of

ORGANIZING FOR INFORMATION OPERATIONS WITHIN
THE JOINT TASK FORCE

Information operations (IO) continue to rise in prominence as a force

multiplier for the joint force. Joint doctrine defines information operations as a broad

range of capabilities and related activities that include operations security,

psychological operations, electronic warfare, physical attack/destruction and special

information operations. Given the importance and scope of IO across the spectrum of

conflict, it would be logical that a robust organizational structure would be prescribed

to support the multiple functions of IO and ensure the necessary coordination required

to implement a comprehensive IO campaign. Unfortunately, this is not the case.

Joint doctrine inadequately integrates IO into the Joint Task Force (JTF) organization

to address the many aspects of IO. The current doctrinal organization for the conduct

of IO – the IO cell – does not provide for unity of command or centralized planning

necessary to support the commander's IO effort. A potential solution to this problem

is to create a new organization within the JTF command and control structure

modeled after the Joint Psychological Operation Task Force (JSOTF). This would

greatly increase the ability of the Joint Force Commander to plan and execute a

comprehensive IO campaign that is integrated with, and complementary to, the

overall campaign plan.

INTRODUCTION

> In order to conquer that unknown which follows us until the very
> point of going into action, there is only one means, which consists in
> looking out until the last moment, even on the battlefield, for *information*.
>
> Marshal of France Ferdinand Foch
> *Precepts and Judgments*, 1919

The concept of information operations (IO) permeates the United States' military culture. Information operations, information warfare, command and control warfare, cyberwar, netwar, network-centric warfare – all of these terms have entered the military lexicon and have made the military establishment relook at how operations are conducted across the spectrum of conflict. Lately, information operations appear to be discussed more than any other military topic to include traditional functions such as logistics, intelligence, and even combat operations. General Ronald Fogleman, former Air Force Chief of Staff, has even described information operations as the fifth dimension of warfare.[1]

A quick review of joint and service publications clearly reveals the high level of interest IO is receiving in all parts of the military community. *Joint Vision 2020* describes information superiority, the result of well planned and executed information operations, as "a key enabler of the transformation of the operational capabilities of the joint force…."[2] *Joint Vision 2020* further states that, "… information operations may evolve into a separate mission area requiring the Services to maintain appropriately designed organizations and trained specialists. Improvements in doctrine, organization, and technology may lead to decisive outcomes resulting primarily from information operations."[3] Service documents provide similar views. The Air Force Doctrine Document 2-5, *Information Operations*, states, "Information operations are integral to all

successful air and space operations."[4] The U.S. Army has recently created a new

functional area, Information Officer, to plan, integrate, and execute IO across the

spectrum of conflict.[5] Lastly, the Department of the Navy in its *Naval Transformation*

Roadmap, Power and Access...From the Sea, lists IO as a "Sea Strike Transformational

Capability."[6] Information Operations, and the resultant information superiority, is fast

becoming more and more important across all levels of warfare and will only increase in

importance as the United States continues to make strides forward in information

technologies and as our adversaries also advance with the proliferation of these

technologies.

     Given the increasing importance and growing potential of information operations

in wartime, it would be logical that a robust organizational structure would be prescribed

to support the multiple functions of IO and ensure the necessary coordination required to

implement a comprehensive IO campaign. Unfortunately, this is not the case. Joint

doctrine inadequately integrates IO into the joint task force (JTF) organization. A

potential solution to this problem is to create a new organization within the JTF command

and control structure modeled after the joint psychological operation task force (JPOTF).

This would greatly increase the ability of the Joint Force Commander to plan and execute

a comprehensive IO campaign that is integrated with, and complementary to, the overall

campaign plan. To understand how a new IO organization would benefit the warfighter,

a brief summary of the scope of what constitutes information operations and a review of

the current doctrinal organization for IO is provided. This analysis will form the basis for

examining the deficiencies of the current IO doctrine. Last, this paper reviews how a

JPOTF type organization can help correct those deficiencies.

IO DEFINED

Although information in warfare has been written about since at least the time of Sun Tzu, IO as it relates to current military operations – a possible separate and distinct form of warfare – is a relatively immature concept. Given its immaturity, IO has not yet developed into a completely homogeneous concept. Only limited consensus has been reached as to what ultimately will constitute IO. The purpose of this paper is not to debate what comprises IO, but to examine the organization that supports it. Therefore, the definition and composition of IO as defined in joint doctrine, specifically Joint Publication (JP) 3-13, *Joint Doctrine for Information Operations*, will be the basis for this analysis.

JP 3-13 states, "Information Operations involve **actions taken to affect adversary information and information systems** while defending one's own information and information systems."[7] The broad concept of information operations in a military context is implemented through the integration of a variety of capabilities and related activities. These capabilities and related activities are divided into two major subdivisions: offensive IO and defensive IO. Generally, offensive IO deal with the adversary's information while defensive IO deal with one's own information, although most capabilities and activities overlap between the two.[8]

Offensive IO, designed to affect adversary decision makers can include, but are not limited to, operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), physical attack/destruction, special information operations (SIO), and in some cases computer network attack (CNA).[9] With the exception of SIO and CNA, all the activities above are traditional applications of military

force and require no further review. Special information operations, on the other hand, are defined in JP 3-13 as those activities, which due to their sensitivity, potential impact, security requirements, or risk, require special review and approval. This could apply to almost anything. CNA are activities to disrupt, deny, degrade, or destroy computers and computer networks or the information they contain. [10]

Defensive IO, intended to protect one's own information, can include, but are not limited to, information assurance (IA), OPSEC, physical security, counterdeception, counterpropoganda, counterintelligence (CI), EW, and SIO. Furthermore, offensive IO supports defensive IO.[11]

At first glance, the list may seem small and mostly comprised of activities that have been part of military operations for centuries, yet the difficulties and complexity of the IO components cannot be underestimated in the ever increasing information-centric U.S. military. For example, military deception can involve very complex activities requiring the highest levels of coordination and integration into the overall strategic and operational plans. Probably the greatest military deception in modern military history is Operation BODYGUARD – the cover and deception plan for the Allied invasion of France during World War II. Operation BODYGUARD contained as many as thirty-six subordinate plans and associated stratagems to conceal from the Germans both the location and time of the invasion. [12] Not only did the deception involve a fake Army led by General Patton, but it also involved co-opting numerous double agents, leaking information in subtle and indirect ways to the enemy, inventing fictitious communications for an entire Allied army, active cooperation with the Russians, and, most importantly, direct involvement by General Eisenhower himself. [13] Imagine the

difficulty of this operation in today's environment, with CNN, the internet, and foreign satellites reporting on a military's every move. Deception is not the only complex IO activity.

Electronic Warfare (EW) in today's combat environment requires a similar effort of coordination and integration. EW is divided into three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).[14] Just EA requires extensive coordination to prevent or reduce electronic fratricide. This is especially critical as the United States involves itself more and more in coalition warfare. The diverse nature of communications hardware and frequencies among numerous coalition partners make the situation truly difficult, especially if a coalition partner is using the same systems as the enemy. The *Operation Allied Force After-Action Report* listed the management of the electromagnetic spectrum and mutual interference as an essential key area of concern.[15]

PSYOP is another pillar of IO that must be coordinated and integrated at the highest levels to ensure consistent themes that conform to national statutory policies, treaties, and agreements.[16] Not only are consistent themes paramount to a successfully integrated PSYOP campaign, numerous assets from the Army, Air Force, Navy, and Special Operations Command will need to be closely coordinated to deliver a variety of PSYOP products from radio and television messages to leaflets dropped from fighter and transport aircraft. PSYOP in Desert Shield/ Desert Storm saw the delivery of over 29 million leaflets from a variety of aircraft, six radio broadcast stations (including two EC-130E aircraft), and numerous loudspeakers mounted on helicopters, vehicles, and carried by individual soldiers.[17]

Individually, the pillars of IO are quite complicated. For an effective IO campaign, all of the various aspects of IO must be integrated together to ensure a consistent and synergistic effort. For example, PSYOP, military deception, and public affairs (PA) all involve releasing information to the enemy, yet for very different purposes and by very different means. If not closely coordinated, a PA release could jeopardize an entire deception or PSYOP campaign. With any PSYOP or deception plan, the 'correct' information has to get to the enemy; therefore, the EW plan has to be coordinated so that the mode of transmission is still functioning and not destroyed or degraded. This is a complicated process that requires considerable effort from a variety of agencies and personnel. Only through a sound organizational structure can the JTF commander hope to conduct an effective IO strategy.

IO ORGANIZATION

If properly organized, the potential of information operations on and off the battlefield is tremendous. As with any military requirement, IO requires the establishment of an organizational structure with the capacity to synchronize and control all aspects of information operations, ensuring continuity of effort. Considering the importance of IO and the plethora of tasks falling under the information operations umbrella, a robust organizational structure is expected within the warfighting staff. Unfortunately, a review of JP 3-13 reveals a doctrinal organization for the conduct of IO in the JTF that lacks the necessary structure and composition to address the scope and complexity of IO.

In accordance with the JP 3-13, the development, prioritization, planning, coordination, deconfliction, and execution of IO are the responsibility of the IO Cell that

is part of, and subordinate to, the J3. The IO Cell is *supervised* by an IO officer,

preferably in the grade of O-6, from the J3 staff.[18] The composition of the IO Cell can

vary with mission requirements, but the Joint Pub does list the composition of a typical

IO Cell to include: [19]

? J-2 Representative	? J-4 Representative
? J-5 Representative	? Public Affairs Officer
? J-6 Representative	? J-7 Representative
? Staff Judge Advocate	? CI Support Officer
? Civil Affairs Representative	? Component Representatives
? OPSEC Program Representative	? Military Deception Representative
? PSYOP Representative	? Targeting Representative
? Special Technical Operations	? EW Officer
? Special Operations Representative	? Other Representatives/LNOs

These representatives form a cell of nineteen individuals from very diverse specialties,

most with different bosses, and with no defined group structure.

    Joint Task Force Planning and Guidance Procedures (JP 5-00.2) lists unity of

effort, unity of command, centralized planning, and common doctrine as essential

elements of sound command organization. [20] Considering the broad scope and

complicated nature of information operations, the elements of sound command

organization are especially relevant. Unity of command dictates that all forces employed

in pursuit of a common purpose operate under a single commander with the authority to

direct those forces.[21] Unity of command is lacking in the IO cell. JP 3-13 implies that

the IO officer only has coordinating authority within the IO cell and with the other

components and agencies of the task force. "Coordinating authority is a consultation relationship…"[22] that only provides the individual with "…the authority to require consultation between the agencies involved but does *not* [emphasis mine] have the authority to compel agreement."[23] Having each IO cell member working for a different boss leaves the whole IO effort resting on voluntary cooperation among organizations within the task force – many with diverse and sometimes competing interests. Therefore, the IO officer has no real authority to ensure a coordinated IO campaign. A counter to this assertion is that unity of command rests with the JTF commander. Although true, the IO campaign needs someone empowered with the authority to ensure that proper coordination, prioritization, planning, and deconfliction occurs across functional and service lines below the level of the JTF commander. The services, especially the Air Force and Army, appear to come much closer to achieving unity of command, unity of effort, and centralized planning in the conduct of their information operations.

The Air Force has a dedicated IO organizational structure within its warfighting component – the information warfare flight (IWF). "The IWF is one of the commander's key IO organizations in the air operation center (AOC) and is one of the main organizational structures through which integrated counterinformation planning and execution are conducted."[24] The IWF resides directly within the AOC, and the core of the information warfare flight consists of experienced information operators from numerous IO disciplines who have no other responsibilities within the AOC. In addition, other members within the AOC may be added to the IWF based on specific expertise or as a liaison with other agencies or organizations.[25] The key points to consider are that the IWF resides in the highest level of the Air Force warfighting structure and consists of a

core of individuals whose only responsibility is the planning, integration, and execution of information operations into the commander's air and space operations.

The U.S. Army has also made great strides in developing a robust organizational structure for the implementation of IO. Besides creating a new functional area for IO within the Army's personnel system, the central focus for IO at the corps level and below is the information operations coordinator (IOCOORD). The IOCOORD is a special staff officer that is responsible for the unity of effort in the corps staff.[26] In addition, the Army's new army field manual (FM 3-13) proposes a 23 person corps information support section with smaller support sections assigned to subordinate combat units.[27]

A review of the Air Force and Army organizations shows a greater emphasis for IO at the service component level than at the JTF level. Although neither the IWF nor the IOCOORD staff directly control assets, both organizations have dedicated and trained individuals at the highest levels of their respective component staffs whose sole function is the conduct of IO to ensure continuity of effort. Conversely, the JTF IO cell has no dedicated staff to ensure the same level of IO effort the Army and Air Force now provide. The IO organization in the joint task force needs to be strengthened, and the solution may be as simple as looking at current organizations already established in the JTF command structure.

A SOLUTION

The current doctrinal organization for the conduct of IO within the JTF staff is inadequate. The question then becomes, what is adequate to address the planning, integration, and execution of IO in joint operations from humanitarian assitance to peacekeeping to major theater wars? Martin Libicki and James Hazlett have even

suggested that the future of IO may require a separate Information Corps with its own culture, doctrine, a separate career field for officer and enlisted personnel, and an associated command structure not subordinate to the other services.[28] An Information Corps may be necessary and feasible sometime in the future, but for the interim a compromise solution is required. The solution needs to elevate IO in the JTF staff to the level of importance that it deserves without separating it from the other military functions upon which its successful implementation so heavily depends. Modeling the IO organization within the JTF after the joint psychological operations task force provides a workable compromise.

According to current doctrine, PSYOP is a subset of IO. Why then would PSYOP have its own organization within the JTF staff, with dedicated personnel whose primary duties are to plan, coordinate, and execute the PSYOP portion of an operation, yet the organization of the larger and more comprehensive information campaign relies on an IO cell operating within the J3 staff? It appears obvious that IO should be elevated to a status as high as, if not higher, than that of PSYOP within the JTF. Beyond the obvious, there are a few distinct reasons why the JPOTF concept would be a very good fit for the organization of IO.

With the current organizational structure for IO, there is no clear line of responsibility and authority for the planning and execution of the IO campaign. Establishing a JPOTF type organization for IO would put one person in charge – directly responsible to the JTF commander for the conduct of the IO campaign – with a staff focused only on the IO effort. Information operations would have a true 'boss'. Under the current doctrinal command relationships for a JTF, the JPOTF does not work directly

under the staff directorates, the functional, or service commands. Instead, the JPOTF works directly for the JTF commander, theoretically, the same as the Joint Force Land Component Commander, Joint Forces Air Component Commander, etc …[29]

Second, the JPOTF is a doctrinally accepted organization within the JTF that has proven effective in operations as far back as Desert Shield/Desert Storm. Like PSYOP, all aspects of IO must begin at the earliest stages of operational planning and should include all available resources – strategic, operational, and tactical.[30] Only by having dedicated personnel under a single commander will this be able to occur. Operation Allied Force showed the true benefit of a JPOTF. LtCol Paul Bowman, Deputy Chief of the Information Operations Division at HQ, U.S. European Command and leader of the IO effort during Allied Force, recounts how the JPOTF was able to stand up prior to Operation Allied Force and start planning and employment activities early. Conversely, the IO cell stood up with only six people once the JTF was established and could not cope with the coordination and execution actions required of the operation.[31] Bowman further states, "The need for close coordination with targeting and intelligence requires far more than a cell one-deep in each key capability, and we discovered the need for expertise in intelligence, comm. /computer, and targeting that also need to be organic to the IO cell."[32] For IO to be truly effective, the task force commander cannot afford to wait until the entire staff is assembled, IO cell members designated, meeting times established and deconflicted, and an agreement reached among the cell members, before information operations get underway. IO has to be planned early, and the personnel tasked to conduct the IO campaign have to be able to 'hit the ground running' in order to be a force multiplier from start to finish.

Although the basic structure of the JPOTF could be employed in the larger IO campaign, changes would have to be made. Since IO includes not only PSYOP, but also military deception, OPSEC, EW, physical attack/destruction, SIO, and CNA, the organization would have to grow significantly to handle the planning and execution of each diverse specialty. Also, intelligence and communications personnel would have to be organic to the IO organization to ensure the necessary support of these functions. A bigger staff would create problems as the Services try to decrease the tooth-to-tail-ratio, but the potential payoff of a comprehensive IO campaign would be worth the added resources.

The rank of the commander would also have to be reconsidered. Currently, the JPOTF is normally commanded by an Colonel. An Colonel may be insufficient to ensure that the requirements established in JP 3-13 of coordinating, planning, and executing all aspect of IO, such as setting priorities; determining the availability of IO resources; liaising with component staffs, joint centers, and other governmental and non-governmental agencies.[33] A flag officer would have more influence in the JTF command structure and would have a much better probability of actually carrying out the multitude of functions prescribed in joint doctrine. Much like PSYOP, IO involves complicated legal, diplomatic, and political concerns that require oversight at the highest levels of the U.S. government. A high-ranking officer leading the IO campaign ensures access to the JTF commander, and therefore, the ability to get the job done.

Of course, IO cannot operate in a vacuum. Should information operations become its own task force within a larger joint task force, coordination with the other components of the JTF will have to be the top priority. Like the JPOTF, the IO

organization will not 'own' the aircraft that drop the leaflets, put steel on target, or jam

the enemy's electromagnetic spectrum, but it will be allocated sorties to support the IO

plans. Similarly, a close relationship with intelligence assets will have to be maintained.

JP 3-13 states that, "intelligence support is critical to the planning, execution, and

assessment of IO."[34] IO personnel will have to leverage the whole of the intelligence

community in the JTF, as well as assets outside of the JTF to be effective. Any new IO

organization must avoid 'stove-piping' its operations. The JPOTF concept has proven

that the required coordination that must exist for the IO campaign can exist.

CONCLUSION

> Normally, there is no ideal solution to military problems; every course has its advantages and disadvantages. One must select that which seems best from the most varied aspects and then pursue it resolutely and accept the consequences. Any compromise is bad.
>
> Field Marshal Erwin Rommel
> *The Rommel Papers*, 1953

Information operations are becoming an increasingly important aspect of

military operations. IO can provide the commander with a potent advantage that

can facilitate rapid military successes with the potential of minimizing casualties,

but the effective conduct of IO is not easy. PSYOP, OPSEC, EW, military

deception, physical attack, SIO, and CNA are all complex activities. Trying to

plan and integrate these various aspects of IO to achieve synergistic effects is

even more daunting. The current organization for the conduct of IO in the joint

task force (the IO cell) is inadequate to plan, coordinate, execute, and assess an IO

campaign given the scope of IO capabilities in the United States' modern military.

Although the IO cell may be able to achieve some unity of effort, the lack of a

dedicated and trained staff under a single command authority responsible for the conduct of IO virtually assures that unity of command and centralized planning – both critical to IO success – will not be achieved. A potential solution to this problem is to develop an IO organization within the JTF similar to the JPOTF.

It seems logical that if the JPOTF works for PSYOP, a subcategory of IO, that it would work for the IO as well. An IO task force would provide, like the JPOTF, the centralized planning and command authority essential to a coordinated IO effort. Since the JPOTF is already a doctrinally accepted organization, the transition to an IO task force should not be difficult. Although an increase in manpower would be required and a review of the rank of the commander would be warranted, the JPOTF template is a definite step forward in bringing IO to the level of importance it requires and deserves.

Notes

[1] Ronald R. Fogleman, "Information Operations: The Fifth Dimension of Warfare," *Defense Issues* 10, no. 47 (1995): 1.

[2] Chairman of the Joint Chiefs of Staff. *Joint Vision 2020* (Washington, DC: U.S. Government Printing Office: June 2000), 3.

[3] Ibid., 30.

[4] U. S. Air Force, *Air Force Basic Doctrine,* Air Force Doctrine Document 1 (Washington, DC: September 1997), vi.

[5] *Information Operations Primer* (Carlisle Barracks, PA: Army War College, January 2001), 25.

[6] U.S. Navy Department, *Naval Transformation Roadmap. Power and Access…From the Sea* (Washington, DC: July 2002), 2.

[7] Joint Chiefs of Staff, *Joint Doctrine for Information Operations,* Joint Pub 3-13 (Washington, DC: 9 October 1998), vii.

[8] Ibid., I-10.

[9] Ibid.

[10] Ibid., GL-5.

[11] Ibid., I-10.

[12] Anthony C. Brown, *Bodyguard of Lies* (New York: Bantam, 1975), 434.

[13] Ibid., 435.

[14] Joint Pub 3-13, II-5.

[15] U.S. Department of Defense, *Report to Congress: Kosovo/Operation Allied Force After-Action Report* (Washington, DC: 31 January, 2000), 27.

[16] Joint Chiefs of Staff, *Doctrine for Joint Psychological Operations,* Joint Pub 3-53 (Washington, DC: 10 July 1996), vi.

[17] U.S. Special Operations Command. *Psychological Operation During Desert Shield/ Storm: A Post-operational Analysis* (MacDill AFB, FL: November 1993), 4-8 – 4-14.

[18] Joint Chiefs of Staff, *Joint Task Force Planning Guidance and Procedures,* Joint Pub 5-00.2 (Washington, DC: 13 January 1999), VII-7.

[19] Joint Pub 3-13, IV-3.

[20] Joint Pub 5-00.2, II-1.

[21] Joint Chiefs of Staff, *Unified Action Armed Forces (UNAAF),* Joint Pub 0-2 (Washington, DC: 10 July 2001), III-1.

[22] Ibid., III-12.

[23] Ibid., III-11.

[24] U. S. Air Force, *Information Operations,* Air Force Doctrine Document 2-5 (Washington, DC: 4 January 2002), 53.

[25] Ibid., 54.

[26] U.S. Department of the Army, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (Approved Final Draft), Field Manual 3-13 (Washington, DC: 21 October 2002), 1-1.

[27] *Information Operations Primer*, 26.

[28] Martin C. Libicki and James A. Hazlett, "Do We Need An Information Corps?," *Joint Force Quarterly*, no. 2 (1993): 88.

[29] For a graphical representation of the command relationship for the JPOTF within a Joint Task Force see JP 3-53, page III-5.

[30] Joint Pub 3-13, V-1.

[31] Paul Bowman, "Information Operations: Strategy or Mission? Reflections on Allied Force," *Cyber Sword* 5, no. 1 (2001): 20.

[32] Ibid., 21.

[33] See JP 3-13, page IV-4, for a complete list of IO officer functions.

[34] Joint Pub 3-13, viii.

Selected Bibliography

Brown, Anthony C. *Bodyguard of Lies.* New York: Bantam, 1975.

Bowman, Paul. "Information Operations: Strategy or Mission? Reflections on Allied Force." *Cyber Sword* 5, no. 1 (2001): 18-21.

Chairman of the Joint Chiefs of Staff. *Joint Vision 2020*. Washington, DC: U.S. Government Printing Office: June 2000.

Eassa, Charles, N. "U.S. Armed Forces Information Operations – Is the Doctrine Adequate." Fort Leavenworth, Kansas: School of Advanced Military Studies, U.S. Army Command and General Staff College, 2000.

Fairbanks, Walter P. *Information Superiority: What Is It? How to Achieve It?* Cambridge, MA: Harvard University, Program on Information Resources Policy, Center for Information Policy Research, June 1999.

Fogleman, Ronald R. "Information Operations: The Fifth Dimension of Warfare." *Defense Issues* 10, no. 47 (1995): 1-3.

Franz, George J. "Information – The Fifth Element of Combat Power." Fort Leavenworth, Kansas: School of Advanced Military Studies, U.S. Army Command and General Staff College, 1996.

Henning, Paul R. "Air Force Information Warfare Doctrine: Valuable or Valueless?" Maxwell AFB, AL: Air Command and Staff College, March 1997.

Information Operations Primer. Carlisle Barracks, PA: Army War College, January 2001.

Libicki, Martin C. *What Is Information Warfare?* Washington, DC: National Defense University, 1995.

Libicki, Martin C., and James A. Hazlett. "Do We Need An Information Corps?" *Joint Force Quarterly*, no. 2 (1993): 88-97.

Strawn, James C. "Information Operations Challenges." Carlisle Barracks, PA: Army War College, April 1998.

Tsouras, Peter G. *Warriors Words: A Quotation Book*. London: Arms and Armour Press, 1992.

U. S. Air Force. *Air Force Basic Doctrine.* Air Force Doctrine Document 1. Washington, DC: September 1997.

_____. *Information Operations.* Air Force Doctrine Document 2-5. Washington, DC: 4 January 2002.

U. S. Department of Defense. *Information Superiority: Making the Joint Vision Happen.* Washington, DC: 2000.

_____. *Report to Congress: Kosovo/Operation Allied Force After-Action Report.* Washington, DC: 31 January, 2000.

U.S. Department of the Army. *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (Approved Final Draft). Field Manual 3-13. Washington, DC: 21 October 2002.

U. S. Joint Chiefs of Staff. *Doctrine for Joint Psychological Operations.* Joint Pub 3-53. Washington, DC: 10 July 1996.

_____. *Joint Doctrine for Information Operations.* Joint Pub 3-13. Washington, DC: 9 October 1998.

_____. *Joint Doctrine for Military Deception.* Joint Pub 3-58. Washington, DC: 31 May 1996.

_____. *Joint Task Force Planning Guidance and Procedures.* Joint Pub 5-00.2. Washington, DC: 13 January 1999.

_____. *Unified Action Armed Forces (UNAAF).* Joint Pub 0-2. Washington, DC: 10 July 2001.

U.S. Navy Department. *Naval Transformation Roadmap. Power and Access…From the Sea*. Washington, DC: July 2002.

U.S. Special Operations Command. *Psychological Operation During Desert Shield/ Storm: A Post-operational Analysis*. MacDill AFB, FL: November 1993.